IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

SECURE DATA TECHNOLOGIES, INC.	)	
	)	
Plaintiff	)	
	)	
v.	)	CASE NO. 4:20-1228
	)	
JAMIE STEPHANIE GUILFORD	)	
	)	
&	)	
	)	
GUILFORD TECHNOLOGIES, LLC	)	
	)	
	)	JURY DEMAND
	)	
Defendants	)	

COMPLAINT

The Parties

1. Plaintiff Secure Data Technologies, Inc. (referred to herein as "Secure Data" and "Plaintiff") is an Illinois Corporation and citizen with its primary place of business located at 1392 Frontage Road, O'Fallon, St. Clair County, Illinois.

2. Defendant Jamie Stephanie Guilford (referred to herein as "Guilford") is a resident and citizen of Missouri, 856 Autumn Grove Dr., O'Fallon, Missouri 63365.

3. Defendant Guilford Technologies, LLC ("hereto refereed as Guilford Technologies") is a Missouri Limited Liability Corporation, a citizen of the State of Missouri, formed in May, 2020, with its primary place of business located at 856 Autumn Grove Dr., O'Fallon, Missouri 63365. Defendant Jamie Guilford is its CEO and registered agent.

Nature of the Action

4. This civil action is for Breach of Contract (Count I), Tortious Interference with Plaintiff's Contracts and/or Business Expectancies (Count II), Unjust Enrichment (Count III), Misappropriation of Trade Secrets in Violation of the Illinois Uniform Trade Secrets Act, ("ITSA") (765 ILCS 1065/1 *et seq*)). (Count IV), Violations of Stored Wire and Electronic Communications Act ("SECA"), 18 U.S.C. § 2701, *et seq*. (Count V), Violations of Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq*. (Count VI), Violation of the Missouri Statute Against Tampering with Computer Data and Equipment, R.S. Mo. § 537.525, and the Missouri Statute Against Tampering with Computer Equipment, R.S. Mo. § 569.097 (Count VII).

Jurisdiction and Venue

5. This Court has original diversity jurisdiction of the instant matter pursuant to 28 U.S.C.§1332 for it is a civil action where the matter in controversy exceeds the sum or value of $75,000, exclusive of interest and costs, and is between citizens of different States. Plaintiff Secure Data is a citizen of Illinois. Defendants Guilford and Guilford Technologies are Missouri citizens. Additionally, This Court also has federal question jurisdiction over Counts VI and VII of this Complaint, which are claims under the Stored Wire and Electronic Communications Act ("SECA"), 18 U.S.C. § 2701 *et seq*. and the Computer Fraud & Abuse Act ("CFAA), 18 U.S.C.§ 1030 ei *seq*, respectively. This Court has supplemental jurisdiction over the remaining Counts.

6. Venue is appropriate in this Court inasmuch as the Plaintiff and Defendant Guilford resides or otherwise can be found within the District, the subject matter leading to the formation of his consulting business, a Missouri Limited Liability Company, was engaged in by Defendant Guilford within this District, the tampering with a computer occurred within this

district, and the causes of action against Defendant Guilford arise from multiple acts committed by Guilford in Missouri. This Court has personal jurisdiction over the Defendant who is a citizen of Missouri, residing in the Judicial District of the Eastern District of Missouri.

Facts Common to all Counts

7. Plaintiff Secure Data is an infrastructure technology company, which provides clients with hardware, software, managed services and professional services in four areas: Collaboration, Data Center, Network and Security.

8. Defendant Jamie Stephanie Guilford (referred to herein as "Guilford") was a salaried Senior Consulting System Engineer. Part of Guilford's job was to interface with secure data's client base, to work with wireless, security and Data center design, set up and integration.

9. Defendant Guilford Technologies is a direct competitor of Secure Data, formed and maintained by Guilford to provide consultative, infrastructure technology services.

10. Defendant Guilford work for Secure Data from the period of approximately July 9, 2018 to February 23, 2020 (beginning under her previous name Stephen Guilford), and now is employed by Guilford Technologies.

Guilford Illegally Hacked into Company Email

11. During the period of Guilford's employment with secure Data for which she was receiving salary, there were concerns raised within the company that Guilford improperly and without authorization hacked into the email accounts of Secure Data management.

12. Secure Data confirmed that prior to her termination, Guilford improperly and illegally hacked into Secure Data's communications system to review sensitive email exchanged among Secure Data's management team.

13. On the evening of February 23, 2020, Jeff Young of Secure Data was alerted to a possible security breach of Secure Data's email system. Upon reviewing audit logs, Young noticed that Guilford had provided herself unapproved access to the mailboxes of CEO Dana Steffey, CFO Derek Herbison and employee Simonne Meszaros

14. After additional review, Young confirmed that Guilford also accessed Young's own email mailbox without approval on February 21, 2020 and multiple other times the week of February 17, 2020.

15. On the evening of February 23, 2020, Young of Secure Data was alerted to a possible security breach of Secure Data's email system. Upon reviewing audit logs, Young noticed that Guilford had provided herself unapproved access to the mailboxes of CEO Dana Steffey, CFO Derek Herbison and employee Simonne Meszaros

16. After additional review, Young confirmed that Guilford also accessed Young's own email mailbox without approval on February 21, 2020 and multiple other times the week of February 17, 2020.

17. Attached hereto as Exhibit 2 and incorporated herein is an admission by Guilford that she illegally hacked into Secure Data's confidential emails.

18. Guilford was terminated from Secure Data as a result of her improper conduct.

The Non-Compete Agreement

19. Attached hereto as Exhibit 1 is an Employee Non-Compete Agreement entered into by Guilford with Secure Data on June 22, 2018.

20. Section 2 of said Non-Compete Agreement has the following terms in place concerning "Confidential Information":

2. Confidential Information.

(a) From and after the date of this Agreement (without limitation as to time), Employee shall treat as the Company's confidential information ("Confidential Information") all data, customer lists, information, ideas, knowledge and papers pertaining to the affairs of the Company which are not made public under the direction of the Company's management. Without limiting the generality of the foregoing, such Confidential Information shall include: the identity of customers; the identity of the Company's suppliers and prospective suppliers; the identity of the Company's creditors and financial backers or potential creditors and other potential financial backers; technical improvements, designs, inventions, methods, processes, techniques and skills, devised, developed or used by or for the Company; the Company's estimating and costing procedures and the cost and gross prices charged by the Company for its services; the prices or other consideration charged to or required of the Company by any of its suppliers or potential suppliers; and the Company's sales and promotional policies. Employee shall not reveal Confidential Information to others except in the proper exercise of Employee's duties and authority for the Company, nor use Employee's knowledge thereof in any way that would be detrimental to the interests of the Company. Employee shall also treat all information pertaining to the affairs of the Company's customers and suppliers with the same degree of confidentiality as he is obligated to treat the Confidential Information. Employee shall upon or prior to Employee's termination of employment with the Company turns over to the Company all copies of all documents, papers, memoranda, data, or other matter, whether published or unpublished and in whatever media they exist, which Employee may have or control relating to the Company or its customers, and that the same is and shall be the exclusive property of the Company and the Company shall be entitled to all copyright rights therein.

(b) All inventions, designs, discoveries, developments, improvements or other Confidential Information, whether or not patentable or subject to copyright, developed by Employee while an employee of the Company shall belong exclusively to the Company. Without limiting the foregoing, all copyrightable material produced by the Employee while an employee of the Company shall be deemed to be "works for hire" produced for the Company. Employee shall execute such other documents and perform (or cause to be performed) such other acts as the Employer may reasonably request in order to effectuate the provisions and intent of this paragraph and assist the Company in enforcing its rights in said inventions, designs, discoveries, developments, improvements or other Confidential Information.

(c) Employee covenants that Employee has not and will not use or disclose the confidential information of any of Employee's prior employers. Employee covenants that, by Employee's employment by the Company will not violate any agreement that Employee has with any of Employee's prior employers.

21. On March 2, 2020, Secure Data sent a letter via Certified Mail to Guilford, with a copy of the Non-Compete Agreement attached. The letter stated in part:

> Per paragraph 4, you are required to provide a copy of the Agreement to any prospective employer so that any such employer would not inadvertently cause the violation of the Agreement. I have provided a copy of the Agreement, so that you will be able to provide it to any current or prospective employer.
>
> As you can see, Paragraph 1 of the Agreement provides that for a period of one year following your departure from Secure Data, you will (a) not solicit or accept business from any entity that is a past, current or prospective customer of Secure Data; and (b) will not solicit or induce any person to leave the employ of Secure Data. Further, paragraph 2 provides that you will not divulge or use Secure Data's confidential information.

> Your departure date from Secure Data was February 23, 2020. In your time at Secure Data, you acted as an engineer and has had contact with all of Secure Data's clients and had access to Secure Data's customer lists. Per the Agreement, you are to turn over all documents related to his work with Secure Data, including all customer information. Please ensure that you have done so, and that you will not use your knowledge of Secure Data Customers derived from Secure Data's proprietary information while you are either under the employ of any third party or acting as an independent contractor.

Guilford's Access to Confidential Information

22. During her remaining days with Secure Data time period, Guilford had the advantage of reviewing, choosing and storing relevant information to take from Secure Data to use after she departed from Secure Data's employ for the benefit of starting a competitive business.

23. On information and belief, towards the end of her employment, Guilford gained access to the proprietary and confidential internet cloud based information, including Secure Data's information.

24. Said confidential and proprietary information was kept by Guilford for Guilford to use to subsequently offer competing services to Secure Data's customers.

Guilford's Offer of Services to Secure Data's Customer Tacony

25. One of the customers to which Guilford is offering competing services is Tacony Corporation ("Tacony").

26. Tacony was a major client of Secure Data, for multiple years, starting in 2013. In 2019, alone, Secure Data received $ 378,557 in revenue.

27. Guilford was aware of the secure Data/Tacony relationship, and worked with Secure Data on Tacony projects.

28. Guilford maintained and used the Confidential Information related to the Tacony projects after parting from Secure Data, in order to have his newly formed company, Guilford Tachnologies contract with Tacony and offer a competing set of services, based on the original services provided by secure Data.

29. During Secure Data's daily review of their client Tacony's Veeam infrastructure, which is covered under their managed services, Secure Data became aware that some information regarding Jamie Guilford, was *added* after Guilford's departure from Secure Data.

30. When Secure Data attempted to connect to their Veeam server via remote desktop it was observed that a user (main\jguilford) was connected to the machine (jguilford-rdp.jpg).

31. Upon Secure Data's review of the Tacony status of backups it was noticed that new job was created by "main\jguilford" on August 24, 2020 (jguilford-backupjob.png).

32. Upon noticing this job creation Secure Data recalled a ticket (#51168 bundled with ticket #51018) being created in its system on August 26, 2020 for failed jobs. On this ticket Secure Data notified Tacony that Secure Data was looking into this. Tacony's representative responded that the alert issued by Secure Data requested should be disregarded, and that Tacony would work out the issue without Secure Data's involvement.

33. Around the same period of time that the "main\jguilford" data was observed within the Tacony system, Secure Data became aware of a change in the relationship between secure Data and Tacony, which included a loss of expected revenue from the relationship.

COUNT I- Breach of Contract- Guilford

34. Plaintiff incorporates by reference Paragraphs 1 through 33 into this Count I of Plaintiff's Complaint.

35. Guilford's Non-Compete Agreement (Exhibit 1) is a valid and enforceable contract.

36. The confidentiality covenants and other provisions contained in the Non-Compete Agreement are reasonably necessary to protect legitimate protectable interests in trade secrets, confidential information, customer relationships, work force and goodwill.

37. Secure Data has fully performed all of its obligations under the Non-Compete Agreement.

38. Guilford breached and threatens to continue to breach the Non-Compete Agreement in at least one of the following ways by: A. Using an appropriating Secure Data's proprietary and secret data concerning its client Tacony, and other clients; B. by forming a competitor company to use said Confidential information; C. by soliciting clients of Secure Data (including Tacony); D. By entering into service agreements, and being employed by a company that enters into service agreements, with Secure Data's clients (including Tacony) to provide services related to Secure Data's proprietary information and services; E. By using Secure Data's proprietary Information in competition against Secure Data concerning the service of on-going clients of Secure Data; F. by sharing Secure Data's proprietary information with a competitor, Guilford Technologies, for it to compete directly against Secure Data.

39. As a result of anyone of these breaches of the Non-Compete Agreement, Secure Data has been injured and faces additional injury.

40. Secure Data lost and is threatened with losing customers, technology, its competitive advantage, its trade secrets and goodwill.

WHEREFORE, Plaintiff requests that this court issue an order in its favor and against Defendant Guilford as to Guilford's' breach of contract, to award damages concerning said breach, costs, attorneys' fees and all other relief the Court finds appropriate.

Additionally, Plaintiff requests that (a) Defendants be temporarily, preliminarily, and permanently enjoined and restrained as follows: (1) That Defendants will keep at all times confidential and shall not divulge, reveal or disclose any of Secure Data's trade secrets, confidential or proprietary information including, but not limited to, discoveries, patentable and non- patentable ideas, concepts, software in various stages of development, design, drawings, formulae, specifications, techniques, technology, processes, procedures, "know how", marketing techniques and materials, marketing and development plans, customer names and other information related to customers, price lists, pricing policies and financial information, as well as any information described above which Secure Data treats as proprietary or Confidential Information. (2) That Defendants shall return to Secure Data all originals and all copies of documents (electronic or otherwise) that are proprietary, confidential, and/or trade secret information, including trade secrets documents concerning Secure Data's clients, that Defendants obtained, learned, created, or was made aware of during his employment with Secure Data. (3)That Defendants are prohibited from using, relying upon, or disclosing to Guilford Technologies or any affiliate or any other person or legal entity any Trade Secret Information or confidential information of Secure Data acquired by Guilford in the course of or arising out of their employment by Secure Data. (4) For an accounting of all monies and profits realized by Guilford as a result of the conduct alleged herein and for other damages that may be determined and fixed by this Court. (5) For an Order restraining Defendants from duplicating or copying any

of Secure Data's electronic information. (6) For an Order requiring Defendants to immediately return all Secure Data information currently in their possession, whether in electronic or hard copy form.

(b) For monetary damages in an amount equal to the loss sustained by Secure Data as a result of Defendants' misappropriation and wrongful use or disclosure of Secure Data's trade secrets, according to proof at trial, including lost profits to Secure Data;

(c) Punitive damages and for attorney's fees in an amount fair and reasonable under the circumstances and to deter Defendants and others from any continuation, repetition, related misconduct in violation of Secure Data's rights and interests in Secure Data's trade secrets or other electronic information to the extent Defendants engaged in any fraudulent or intentional misconduct; and

(d) For further relief the Court deems just and reasonable.

COUNT II- Tortious Interference with a Contract- Guilford and Guilford Technologies

41. Plaintiff incorporates by reference Paragraphs 1 through 40 into this Count II of Plaintiff's Complaint.

42. Guilford and Guilford Technologies breached and threatens to continue to breach the contract in at least one of its client's (Tacony's) contracts and/or business expectancies.

43. Guilford had knowledge of the agreement and services provided by Secure Data to Tacony based on the Confidential Information he acquired while employed with Secure Data.

44. Guilford and Guilford Technologies used the Confidential Information acquired with Secure Data to contract with Tacony to offer competitive services, directly in contravention with his Non-Compete Agreement.

45. Guilford and Guilford Technologies intentionally and unjustifiably induced breach of the agreement and business expectations that Secure Data shared with Tacony; and Defendants used the Confidential Information received surreptitiously from Secure Data for competitive purposes against Secure Data, in direct violation of the agreement.

46. As a result of the tortious interference with Secure Data's contract and business expectancy with Tacony, Secure Data has been injured and faces additional injury.

47. Secure Data lost and is additionally threatened with losing customer sales and services, its competitive advantage, its trade secrets and goodwill, as result of Guilford and Guilford Technologies' conduct.

48. Guilford's conduct as to the misappropriation of Secure Data's trade secrets in relation to inducing a secretive business agreement with Tacony is contrary to the terms of the agreement Guilford entered into with Secure Data. Said conduct has been willful and malicious, as Guilford's conduct occurred, intentionally surreptitiously, after Guilford was fully cognizant that she was seeking business with Tacony based on ill-gotten competitive information. Therefore, Plaintiffs are entitled to an award of punitive damages.

WHEREFORE, Plaintiff requests that this court issue an order in its favor and against Defendants Guilford and Guilford Technologies as to inducing a breach of contract and/or reduction in business expectancies, to award actual and punitive damages in excess of $ 75,000 concerning said breach, costs, attorneys' fees and all other relief the Court finds appropriate.

COUNT III -Unjust Enrichment

49. Plaintiff incorporates by reference Paragraphs 1 through 48 into this Count III of Plaintiff's Complaint.

50. Defendants will be unjustly enriched by the misappropriation of Secure Data's trade secrets and confidential information, and, unless restrained, will continue to threaten to use, actually use, divulge, and threaten to disclose, acquire and/or otherwise misappropriate Secure Data's trade secrets and confidential information.

51. Defendant's misappropriation has been willful and malicious in light of Guilford's execution of a contract prohibiting his current conduct and his deliberate violation of the contractual obligations, and secretive application and acceptance of a job offer to work for a competitor, and selection, download and use of Secure Data's Confidential Information. Plaintiffs are entitled to an award of punitive damages.

WHEREFORE, Plaintiff requests that this court issue an order in its favor and against Defendants Guilford and Guilford Technologies, to award actual and punitive damages in excess of $ 75,000 concerning said breach, costs, attorneys' fees and all other relief the Court finds appropriate.

COUNT IV- Violation of the Illinois Trade Secrets Act

- Guilford & Guilford Technologies

52. Plaintiff incorporates by reference Paragraphs 1 through 51 into this Count I of Plaintiff's Complaint.

53. Under Illinois law, an employer's trade secrets are a protectable interest.

54. Defendants misappropriated Secure Data's trade secrets in violation of the Illinois Trade Secrets Act ("ITSA") (765 ILCS 1065/1 *et seq*)).

55. The ITSA, in relevant part, provides: `Trade secret' means information, including but not limited to, technical or non-technical data, a formula, pattern, compilation, program, device, method, technique, drawing, process, financial data, or list of actual or potential customers or suppliers that: (1) is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality." 765 ILCS 1065/2(d) (West 2002).

56. Secure Data has expended considerable time, resources and expense to develop and market its products, to develop substantial relationships and goodwill with its customers, suppliers, prospective customers, and brokers, and to develop its goodwill and name.

57. Secure Data considers certain confidential customer, production and business information to be trade secrets (hereinafter "Trade Secret Information"), This Trade Secret Information includes but is not limited to certain reports (which contain specific information regarding customers), customer lists, prospect lists, pricing information, customer preferences, costs and processes, proprietary vendors, profit margins, proprietary processes, and formulae.

58. The Trade Secret Information is not generally known to the public nor readily ascertainable by proper means.

59. The Trade Secret Information, including the confidential customer information contained in the reports was developed at considerable cost and expense over a period of years. It would require, at a minimum, a number of years, and considerable time and expense, to recreate

even a portion of this Trade Secret Information through lawful means. The possession and/or use of such information would give Secure Data's competitors an unfair economic advantage in developing, marketing and selling their products.

60. Secure Data used, and continues to use, reasonable and diligent efforts to maintain the secrecy and protect its Trade Secret Information. These efforts include but are not limited to prohibiting access to the information by the general public, adopting employment policies, including confidentiality, return of property, and electronic media policies, to protect the confidentiality of the Trade Secret Information. In addition, Secure Data maintains extensive security at its facility. Among the steps taken by Secure Data to protect its proprietary customer information was to enter into agreements with all of its sales force to keep such information confidential; to store the information on a limited access computer system, and only allow those who have acknowledged the secret and proprietary nature of the information to use it, and to intentionally not publish the information to the public.

61. The Trade Secret Information derives independent economic value from not being generally known to, and not being readily ascertainable by proper means, by other persons who can obtain economic value from its disclosure or use. By reason of the above, the Trade Secret Information and/or portions thereof, constitute trade secrets within the meaning of the Illinois Uniform Trade Secrets Act.

62. Guilford's Non-Compete Agreement specifically provides "From and after the date of this agreement (without limitation as to time), Employee shall treat as the Company's Confidential Information ('Confidential Information) all data, customer lists, information…and

papers which the company has not made public under the direction of the company's management.

63. Among the Trade Secrets/ Confidential Information taken by Guilford to her new employer, Guilford Technologies, are, *inter alia*, materials specifically deemed confidential under the Non-Compete Agreement, including the identity of its customers (Tacony and others), the Company's estimates and costing procedures and the cost and gross prices charged by Secure Data for its services, and sales and promotional policies.

64. In the instant case, Guilford secretly retrieved and took trade secrets maintained by Secure Data before departing its employment. Prior to her departure, Guilford retrieved from Secure Data's proprietary software system information concerning its customers (Tacony and others).

65. Secure Data has an ascertainable right to the information taken—specifically that the customer lists, bids, service history (to Tacony and others) and sales quotations that Defendants misappropriated.

66. The sales and other related data taken is sufficiently secret to derive economic value, actual or potential, from not being generally known to other persons who can obtain economic value from its disclosure or use.

67. The sales and other related data taken is the subject of efforts that are reasonable under the circumstances to maintain its secrecy or confidentiality.

68. The sales and other related data taken could not be easily acquired or duplicated by others.

69. On information and belief, in her new employment with Guilford Technologies, Guilford through the auspices of Guilford Technologies is calling on the clients and potential clients of Secure Data, and using the competitive information taken.

70. Defendants' willful misappropriation of Secure Data's trade secrets was intentional and motivated by malice and in conscious disregard of Secure Data's rights.

71. Under the ITSA, the statute specifies, "[a]ctual or threatened misappropriation may be enjoined." 765 ILCS 1065/3 (West 2002).

72. Also, under Illinois law, courts may also grant injunctive relief to prevent the inevitable use or disclosure of misappropriated trade secrets.

73. Among other things, there is a real threat Guilford will use Secure Data's information, which includes customer information, including customer service information, pricing and other customer information, to underbid Secure Data.

74. Under the circumstances, there is a danger of irreparable harm and the absence of an adequate remedy at law as to future use of Secure Data's data by Guilford and Guilford Technologies.

75. In this case, plaintiff seeks a preliminary and permanent injunction to prevent further or inevitable disclosure or use of the trade secrets Guilford misappropriated.

76. The data acquired by Guilford will inevitably be used by Defendants to further Guilford Technologies' business interests, to the detriment of Secure Data.

77. Under the circumstances described herein, there is irreparable harm and lack of an adequate remedy concerning the threat of conversion of Secure Data business, including the prospect that Defendants could strategically underbid Secure Data when competing for future

contracts. Secure Data is threatened with losing customers, technology, its competitive advantage, its trade secrets and goodwill in amounts which may be impossible to determine, unless Defendants are enjoined and restrained by order of this Court.

78. The type of competitive losses alleged here often inflict irreparable injury and lack an adequate remedy at law, due to the difficulty in calculating the loss of existing and future business.

WHEREFORE, Plaintiff requests that this court enter a preliminary and permanent injunction against Defendants prohibiting Defendants and their subsidiaries, officers, directors, agents, servants, employees, licensees, successors, and assigns, and those in active concert, from benefiting from the misappropriation of Plaintiffs' trade secrets and against such continued misappropriation of Plaintiffs' trade secrets, and enter preliminary and permanent injunction to prevent the Defendant from gaining competitive advantage through the unlawful misappropriation. Further, Plaintiff requests that this Court enter judgment against Defendants finding that they violated the Illinois Trade Secrets Act; order that Defendants be required to give an accounting of all gains for profit, and advantage derived through the use of the Secure Data's trade secrets; that judgment be entered for Plaintiff and against Defendants for Plaintiff's actual damages in an amount in excess of $ 75,000, for gains, profits, or advantages attributed to Defendants' violation of the Illinois Trade Secrets Act, according to best available proof; award increased and exemplary damages for Defendants' willful misappropriation of Plaintiffs' trade secrets, which was intentional and motivated by malice and in conscious disregard of Plaintiffs' rights; and for all other relief just and available under the circumstances.

COUNT V -VIOLATIONS OF STORED WIRE AND ELECTRONIC COMMUNICATIONS ACT ("SECA"1, 18 U.S.C. § 2701 et. seq.).

79. Secure Data incorporates by reference as if fully restated herein its allegations contained in Paragraphs 1-78 above.

80. 18 U.S.C. § 2701(a) of SECA provides that: "whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section."

81. 18 U.S.C. § 2707 provides a civil cause for any violation of SECA. *See* 18 U.S.C. § 2707(a) ("any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter [18 U.S.C. §§ 2701 *et seq.*] in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, ... which engaged in that violation such relief as may be appropriate").

82. Guilford intentionally accessed without authorization or otherwise exceeded her authorization to access a facility through which an electronic communication service is provided and thereby gained unauthorized access to Secure Data's protected Trade Secret Information.

83. Guilford's actions allowed her to obtain authorized access to electronic communications (specifically Secure Data's Trade Secret Information) while the Information was in electronic storage.

84. Guilford's actions were in violation of SECA, 18 U.S.C. § 2701(a).

85. WHEREFORE, Plaintiff, Secure Data prays for judgment in its favor and against Defendant Guilford as Count V of Plaintiff s Complaint as follows: (a) Enter a temporary, preliminary, and permanent injunction requiring Defendants to return all and not retain any copies of information they unlawfully obtained from Secure Data; (b) Award damages in an amount to be determined at trial; (c) Award attorneys' fees and costs incurred by Secure Data in pursuit of this litigation; and (d) For further relief the Court deems just and reasonable.

COUNT VI - VIOLATIONS OF COMPUTER FRAUD AND ABUSE ACT ("CFAA"), 18 U.S.C. § 1030 et. seq.

86. Secure Data incorporates by reference as if fully restated herein its allegations contained in Paragraphs 1-85 above.

87. Guilford fraudulently or intentionally exceeded her authorization to access Secure Data's protected computers and protected computer network.

88. At the time he engaged in such conduct, Guilford was acting in his own interests and not the interests of Secure Data.

89. Guilford's conduct has damaged Secure Data in the amount of at least $5,000.

WHEREFORE, Plaintiff, Secure Data prays for judgment in its favor and against Defendant Guilford under Count VI of Plaintiffs Complaint as follows:

(a) Defendant be temporarily, preliminarily, and permanently enjoined and restrained as follows: (1) That Defendant will keep at all times confidential and shall not divulge, reveal or disclose any of Secure Data's trade secrets, confidential or proprietary information including, but not limited to, discoveries, patentable and non- patentable ideas, concepts, software in various stages of development, design, drawings, formulae, specifications, techniques, technology, processes, procedures, "know how", marketing techniques and materials, marketing and

development plans, customer names and other information related to customers, price lists, pricing policies and financial information, as well as any information described above which Secure Data treats as proprietary or Confidential Information. (2) That Defendant shall return to Secure Data all originals and all copies of documents (electronic or otherwise) that are proprietary, confidential, and/or trade secret information, including trade secrets documents concerning Secure Data's clients, that Defendant obtained, learned, created, or was made aware of during his employment with Secure Data. (3)That Defendant is prohibited from using, relying upon, or disclosing to Guilford Technologies or any affiliate or any other person or legal entity any Trade Secret Information or confidential information of Secure Data acquired by Guilford in the course of or arising out of their employment by Secure Data. (4) For an accounting of all monies and profits realized by Guilford as a result of the conduct alleged herein and for other damages that may be determined and fixed by this Court. (5) For an Order restraining Defendants from duplicating or copying any of Secure Data's electronic information. (6) For an Order requiring Defendants to immediately return all Secure Data information currently in their possession, whether in electronic or hard copy form.

(b) For monetary damages in an amount equal to the loss sustained by Secure Data as a result of Defendant's misappropriation and wrongful use or disclosure of Secure Data's trade secrets, according to proof at trial, including lost profits to Secure Data;

(c) Punitive damages and for attorney's fees in an amount fair and reasonable under the circumstances and to deter Defendants and others from any continuation, repetition, related misconduct in violation of Secure Data's rights and interests in Secure Data's trade secrets or

other electronic information to the extent Defendants engaged in any fraudulent or intentional misconduct; and

(d) Award of costs associated with Plaintiffs computer investigation; and

(e) For further relief the Court deems just and reasonable.

COUNT VII – COMPUTER TAMPERING

88. Secure Data incorporates by reference as if fully restated herein its allegations contained in Paragraphs 1-88 above.

89. On information and belief, Guilford committed the hacking into Secure Data's email from Missouri.

90. Guilford's hacking of company email and removal from Secure Data's computer system confidential and proprietary and trade secret information in violation of Mo. Rev. Stat. § 537.525.

91. Guilford violated Mo. Rev. Stat. § 537.525 when she tampered with computer data and equipment belonging to the Secure Data, knowing she was without authorization to do so or knowing she was exceeding his authorization to use the computer data and equipment, and having no reasonable grounds upon which to believe that she was so authorized.

92. As a consequence and proximate result of Guilford's tampering with Secure Data's computer system, Secure Data has suffered and will continue to suffer pecuniary loss in the form of actual damages.

93. That, pursuant to Mo. Rev. Stat § 537.525, Secure Data (as the owner of the computer system, network, programs, and data) has the right to bring a civil action against any and all persons who knowingly and without authorization, or without reasonable grounds to

believe that she has such authorization, tampers with computer data, for: (a) Compensatory damages, including any expenditures reasonably and necessarily incurred by the Plaintiff to verify that the computer system, computer network, computer program, computer service, or data was not altered, damaged, or deleted by the wrongful access; and (b) Reasonable attorney's fees.

THEREFORE, Plaintiff, Secure Data, prays for judgment in its favor and against Defendants Hall and Shaw, under Count IV of Plaintiff's Complaint for compensatory damages in an amount fair and reasonable, and for attorney's fees in an amount fair and reasonable, and for further relief the Court deems just and reasonable.

Plaintiffs respectfully request a Jury Trial as to all counts.

Date: September 10, 2020

Respectfully submitted,

AVIGAD LAW, LLC
By: /s/ Joshua M. Avigad
Joshua M. Avigad
IL ARDC # 6224410
225 S. Meramec, Suite 1021
Saint Louis, Missouri 63105
Telephone: (314) 488-2860
Josh@avigadlaw.com

Attorneys for Plaintiff
Secure Data Technologies, Inc.